SURFmap: A network monitoring tool based on the Google Maps API

Rick Hofstede, Tiago Fioreze

University of Twente, The Netherlands
Introduction

• Network monitoring tools provide information about network traffic transiting within a network

• Most available tools lack to provide geographical information about network traffic

• We propose a monitoring tool that allows network managers to visualize network information by using the Google Maps API’s geographical capabilities
Related work

- There are many network monitoring tools available:
  - Wireshark / Tcpdump
  - ntop / NfSen
  - and much more!!!

- Most of these tools lack to provide geographical information about network traffic

- The Google Maps API has potential to be used in the monitoring of network traffic
Our approach

• To overcome the problem of many current network monitoring tools, we have developed SURFmap, which:
  – provides an user-interface based on the Google Maps API
  – adds a geographical dimension to network information
  – uses zoom levels to distinguish between various aspects of network information
SURFmap architecture

- SURFnet database
- GeoCoder
- Database Handler
- Visualization Processor
- Base Page Layout
- IP2Location™ database
- Google Maps API
- SURFmap Web page
Obtaining information from the databases

- Obtain network traffic information from SURFnet database
- Obtain geographical information about network information from IP2Location™ database
Processing information

- Geocode geographical information to get coordinates for each zoom level
- Convert network information into a proper display format
Visualizing network information

- Plot data by using the Google Maps API
  - Markers provide information about end points
    - They show IPv4 addresses and their geographical location
  - Lines provide information about flows
    - They show information about the end points regarding the used ports, their geographical location, the exchanged amount of packets, octets and throughput
SURFmap zoom levels

• SURFmap provides 4 zoom levels:
  1. Country zoom level
  2. Region zoom level
  3. City zoom level
  4. Host zoom level

• Levels depend on information provided by IP2Location™ database
  – Unknown information is geocoded by using last known level of information
Application prototype
Zoom level grouping example
Host zoom level example

<table>
<thead>
<tr>
<th>IP</th>
<th>Flows</th>
<th>Protocol</th>
<th>Port</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>aa.bb.cc.dd</td>
<td>1</td>
<td>TCP</td>
<td>1456</td>
<td></td>
</tr>
<tr>
<td>ee.ff.gg.hh</td>
<td>2</td>
<td>TCP</td>
<td>3244</td>
<td></td>
</tr>
<tr>
<td>ii.jj.ii.jj</td>
<td>2</td>
<td>TCP</td>
<td>7662</td>
<td></td>
</tr>
<tr>
<td>mm.nn.oo.pp</td>
<td>1</td>
<td>TCP</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>qq.rr.ss.tt</td>
<td>2</td>
<td>TCP</td>
<td>62796</td>
<td></td>
</tr>
<tr>
<td>uu.vv.ww.xx</td>
<td>1</td>
<td>TCP</td>
<td>1456</td>
<td></td>
</tr>
<tr>
<td>yy.zz.aaa.bbb</td>
<td>2</td>
<td>TCP</td>
<td>3244</td>
<td>Overijssel</td>
</tr>
<tr>
<td>ccc.ddd.ee.ff</td>
<td>2</td>
<td>TCP</td>
<td>7662</td>
<td>Netherlands</td>
</tr>
<tr>
<td>gg.hhh.iii.jjj</td>
<td>1</td>
<td>TCP</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>kkk.ll.nn.nn</td>
<td>2</td>
<td>TCP</td>
<td>62796</td>
<td></td>
</tr>
<tr>
<td>oo.pp.qq.qq.rrr</td>
<td>2</td>
<td>TCP</td>
<td>636</td>
<td></td>
</tr>
<tr>
<td>sss.ttt.uu.vv</td>
<td>1</td>
<td>TCP</td>
<td>1984</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.xxx.yy.z">www.xxx.yy.z</a></td>
<td>1</td>
<td>TCP</td>
<td>50972</td>
<td></td>
</tr>
</tbody>
</table>

This is a top 13 of largest flows.
Conclusions

• Current monitoring tools lack to provide geographical information about network traffic
• The network monitoring tool prototype presented in this work:
  – allows network managers to visualize network information using the features provided by the Google Maps API
  – adds a geographical dimension to network information
• We are working on a SURFmap plug-in for NfSen
Questions?
Thanks for your attention!

• Contact:
  – Rick Hofstede *(r.j.hofstede@student.utwente.nl)*
  – Tiago Fioreze *(t.fioreze@utwente.nl)*